RSAC 2025 Conference

Many Voices.
One Community.

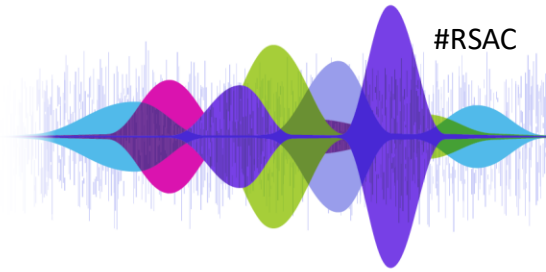
SESSION ID: LAB3-M01

Architectural Thinking for Secure Design

Mark Buckwell
Cloud Security Architect
Security Architecture Consulting
www.linkedin.com/in/buckwem

Carsten Horst
Associate Partner - Cybersecurity
IBM
www.linkedin.com/in/carsten-horst

Stefaan Van daele
CTO NCEE Cybersecurity Services
IBM
www.linkedin.com/in/stefaanvdaele



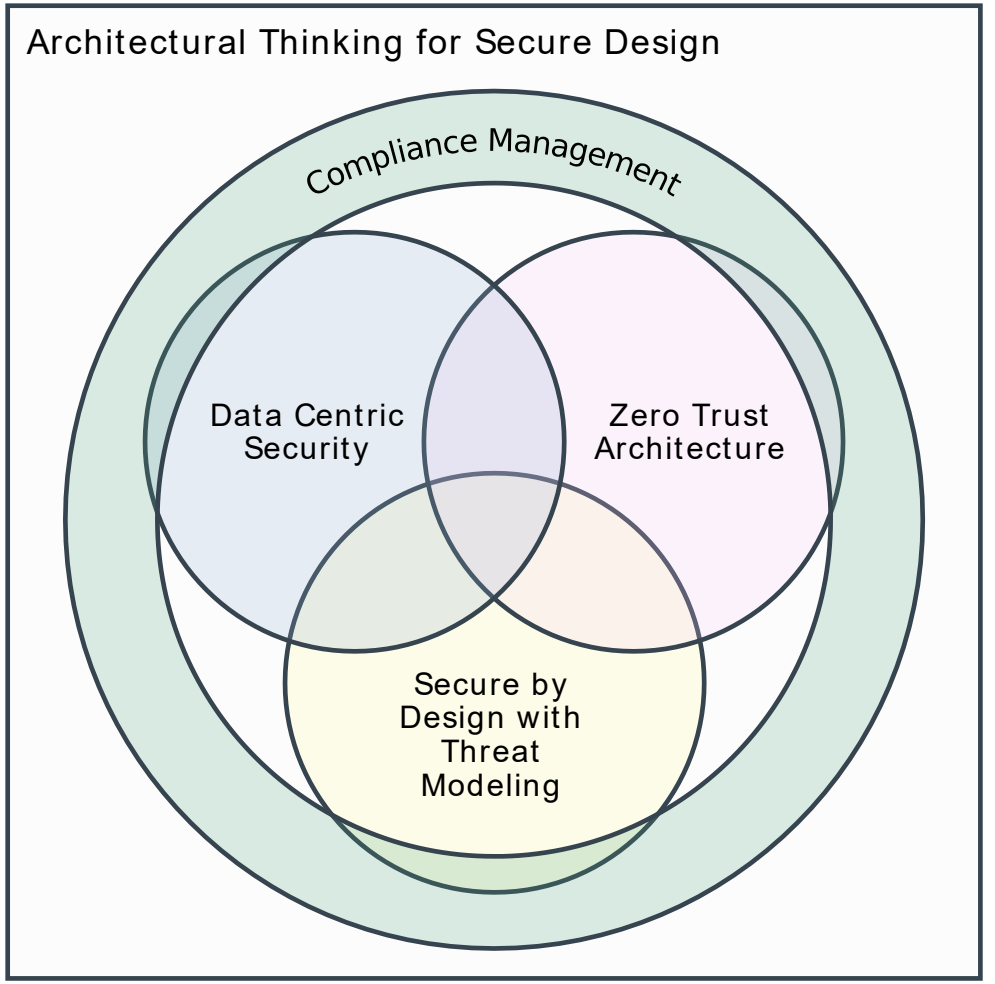
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Architectural Thinking for Secure Design is an integration of different techniques



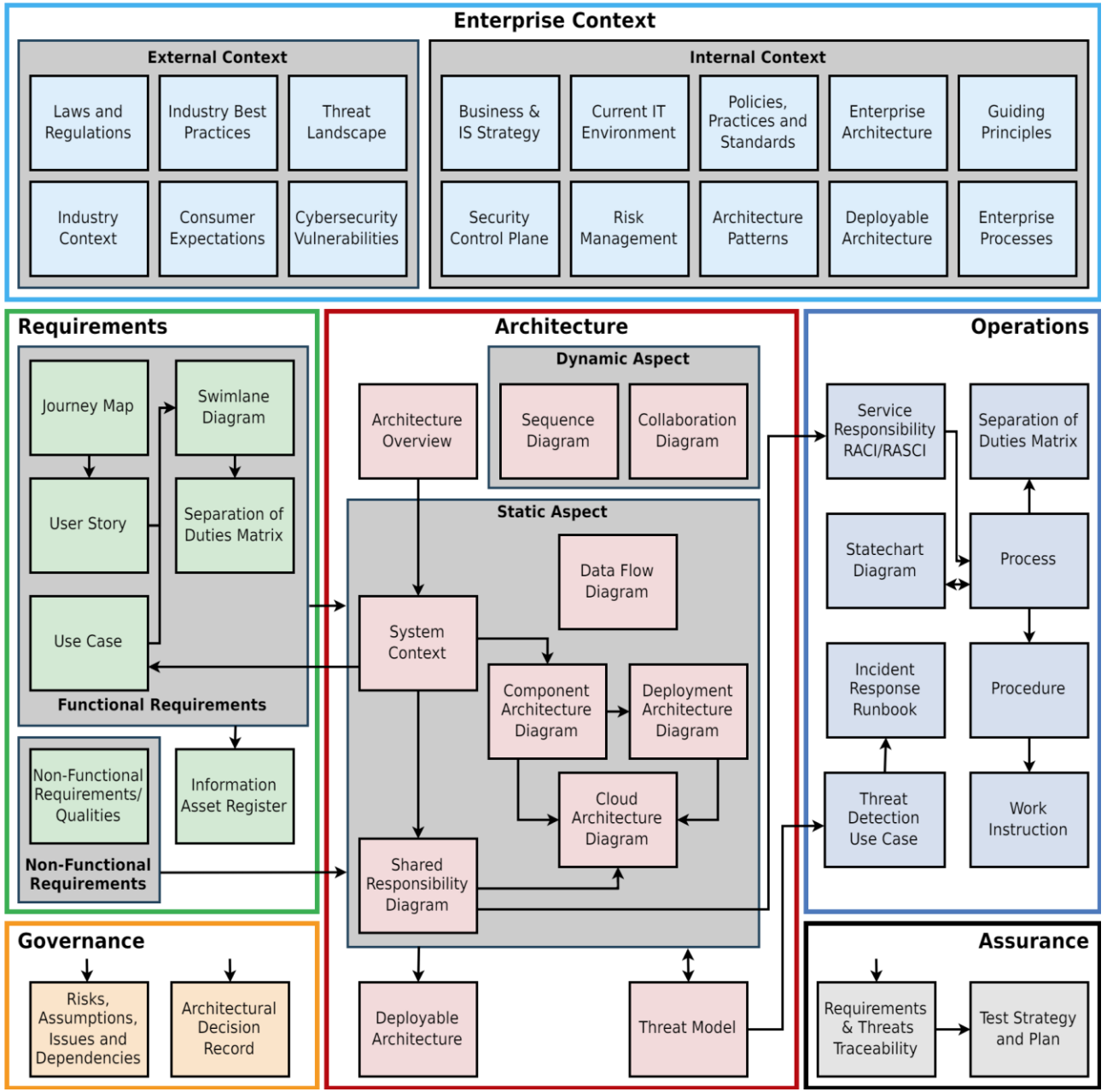
© Mark Buckwell, Carsten Horst and Stefaan Van daele

RSAC 2025 Conference

Stage 1 – Background and Layer 1

Artefact Dependency

We've developed an integrated set of artefacts and techniques

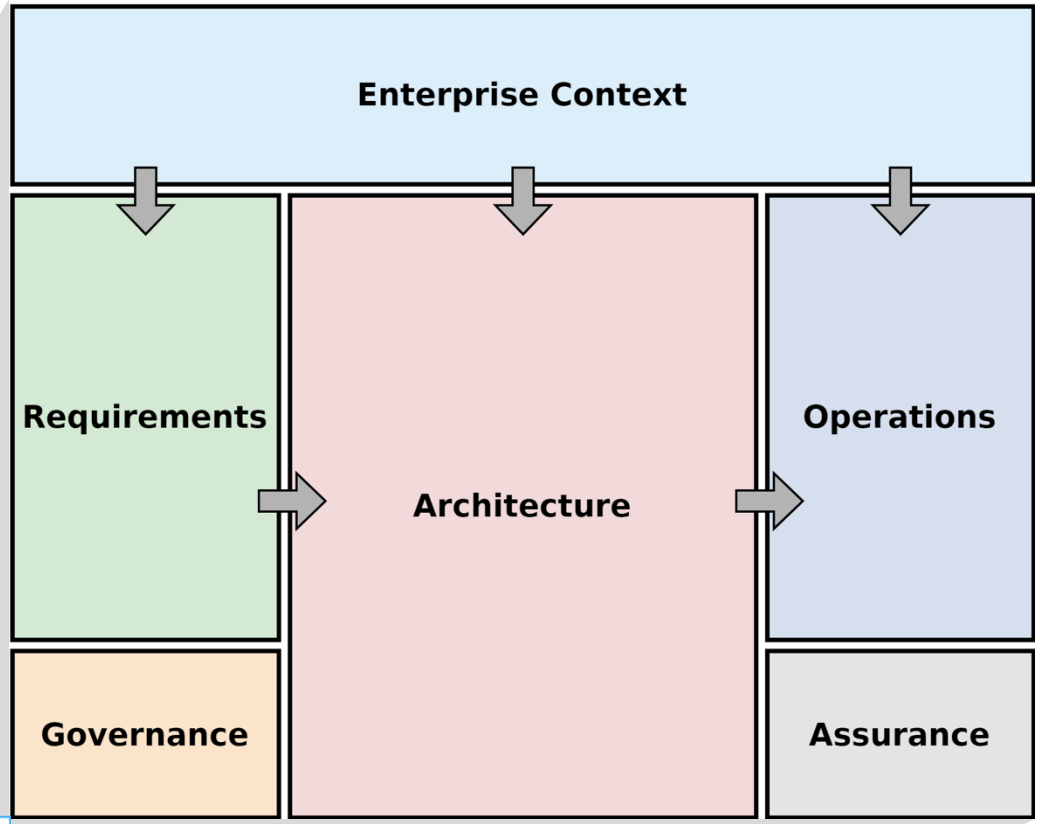


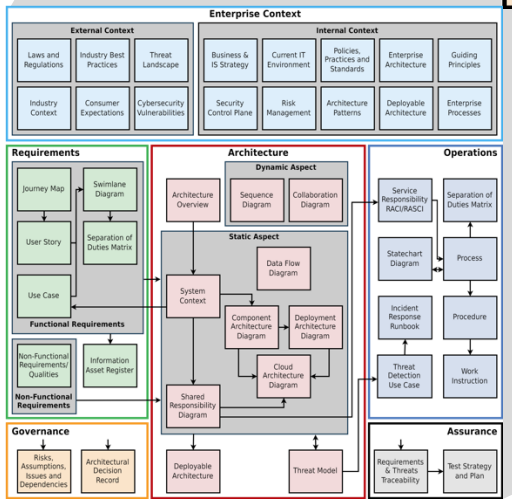
© Mark Buckwell, Carsten Horst and Stefaan Van daele

RSAC 2025 Conference

Artefact Dependency

It’s grouped into stages of architectural thinking

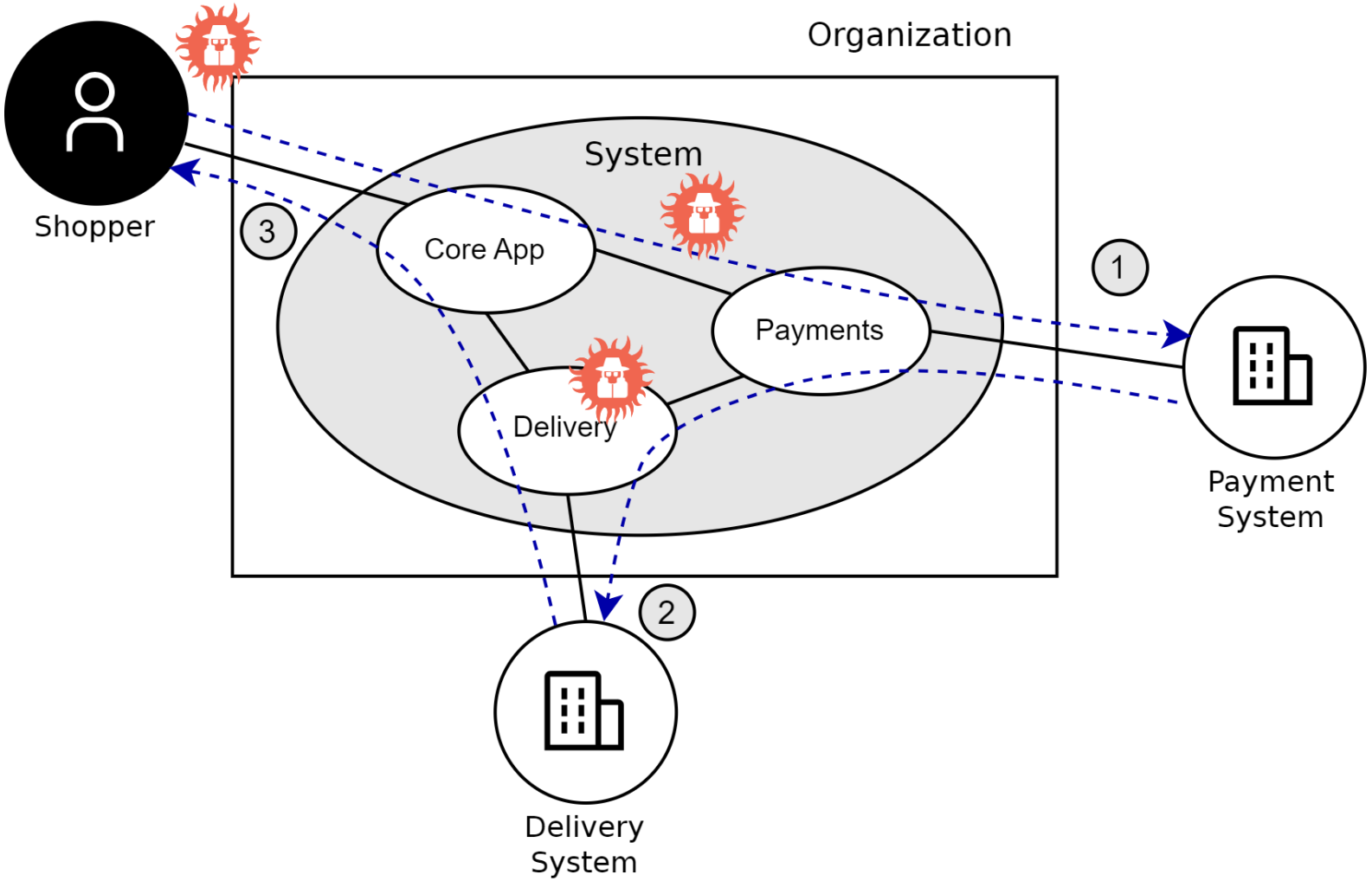




© Mark Buckwell, Carsten Horst and Stefaan Van daele

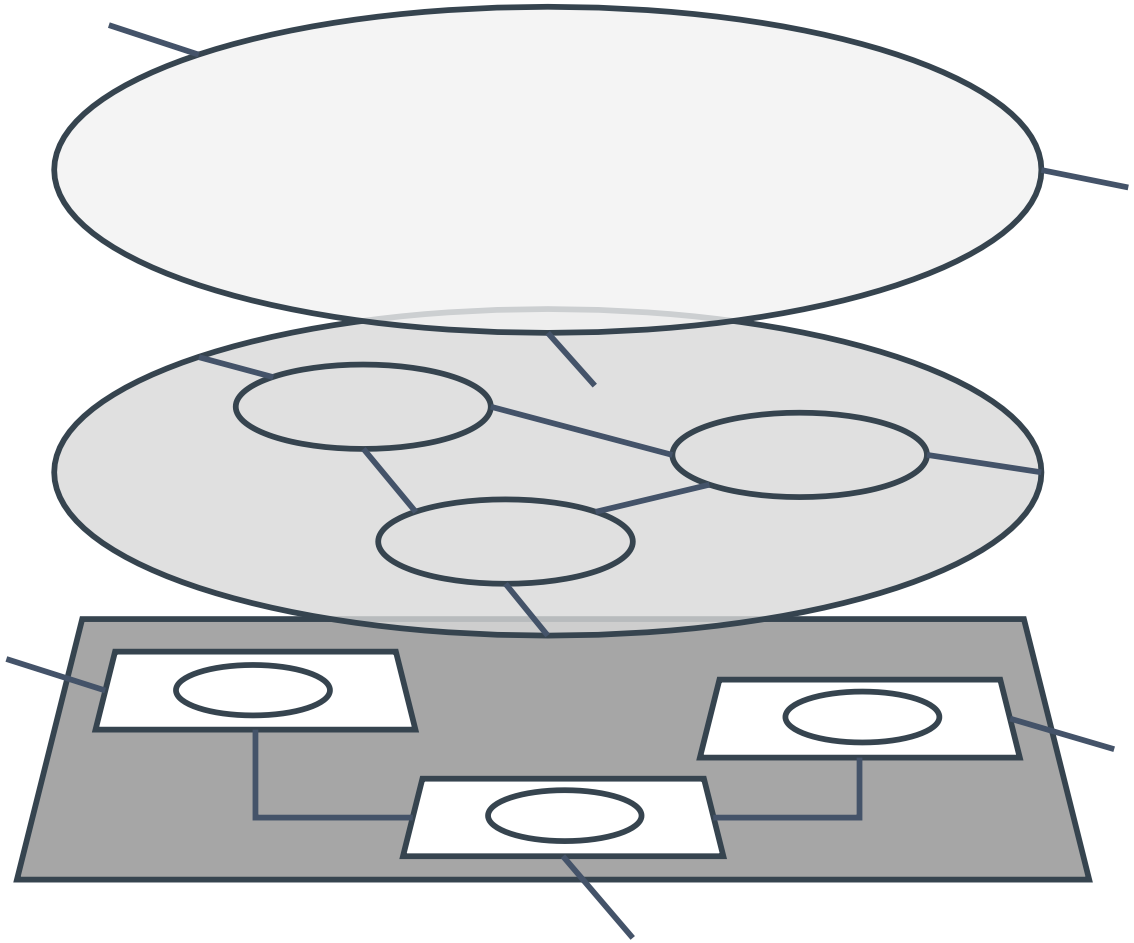
RSAC 2025 Conference

It's all about the threat to data, in transit, at rest and in processing



© Mark Buckwell, Carsten Horst and Stefaan Van daele

The security architecture is developed in layers



System Context

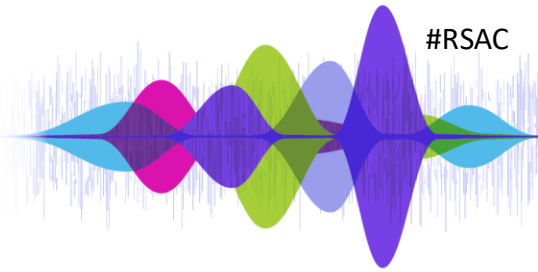
Component Architecture

Deployment Architecture

© Mark Buckwell, Carsten Horst and Stefaan Van daele

#RSAC

RSAC 2025 Conference

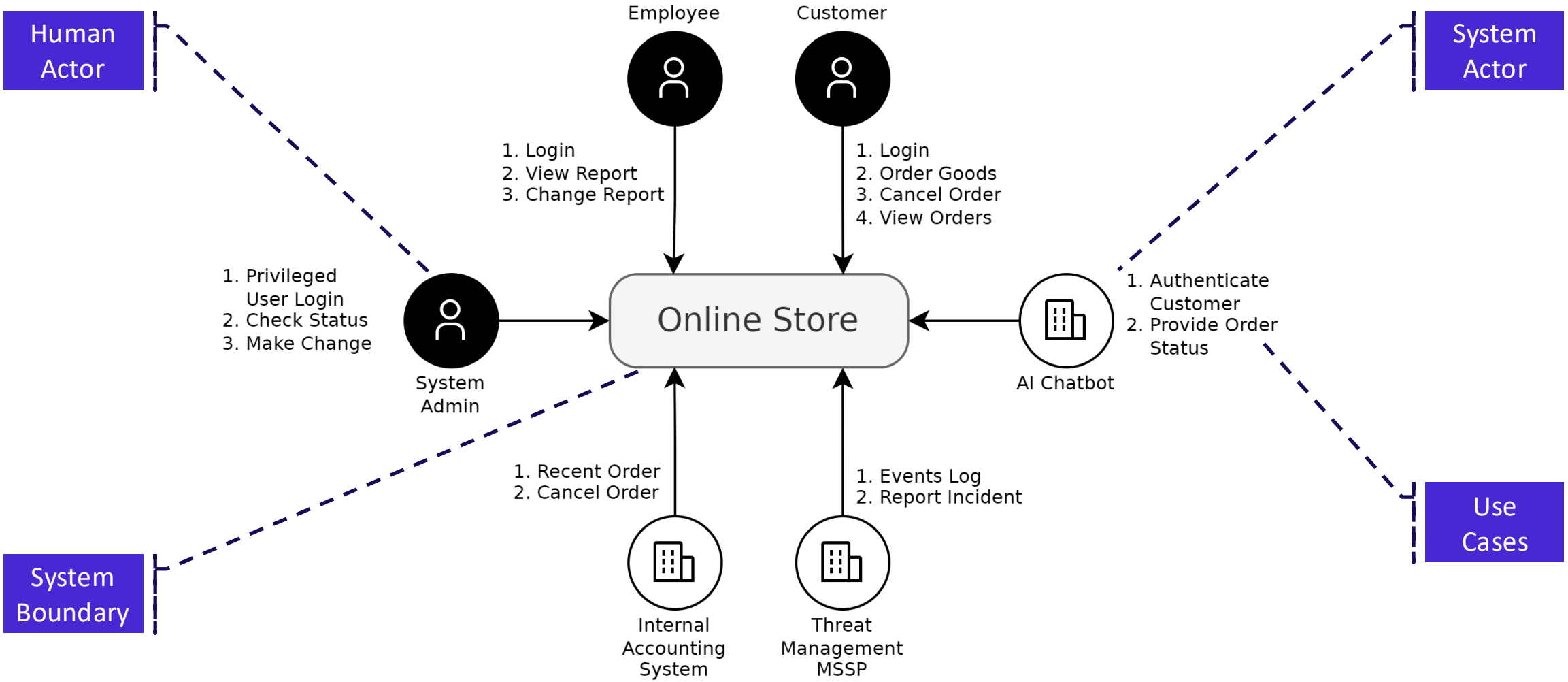


Teams will complete three brief exercises

- Each table will complete three very brief exercises
- Each exercise will touch a layer of architectural thinking
- The exercises will use a case study
- More information on the case study we use can be found at https://securityarchitecture.cloud/rsac/25/case-study

© Mark Buckwell, Carsten Horst and Stefaan Van daele

Understand the boundary of the system and the actors triggering transaction flows to process data

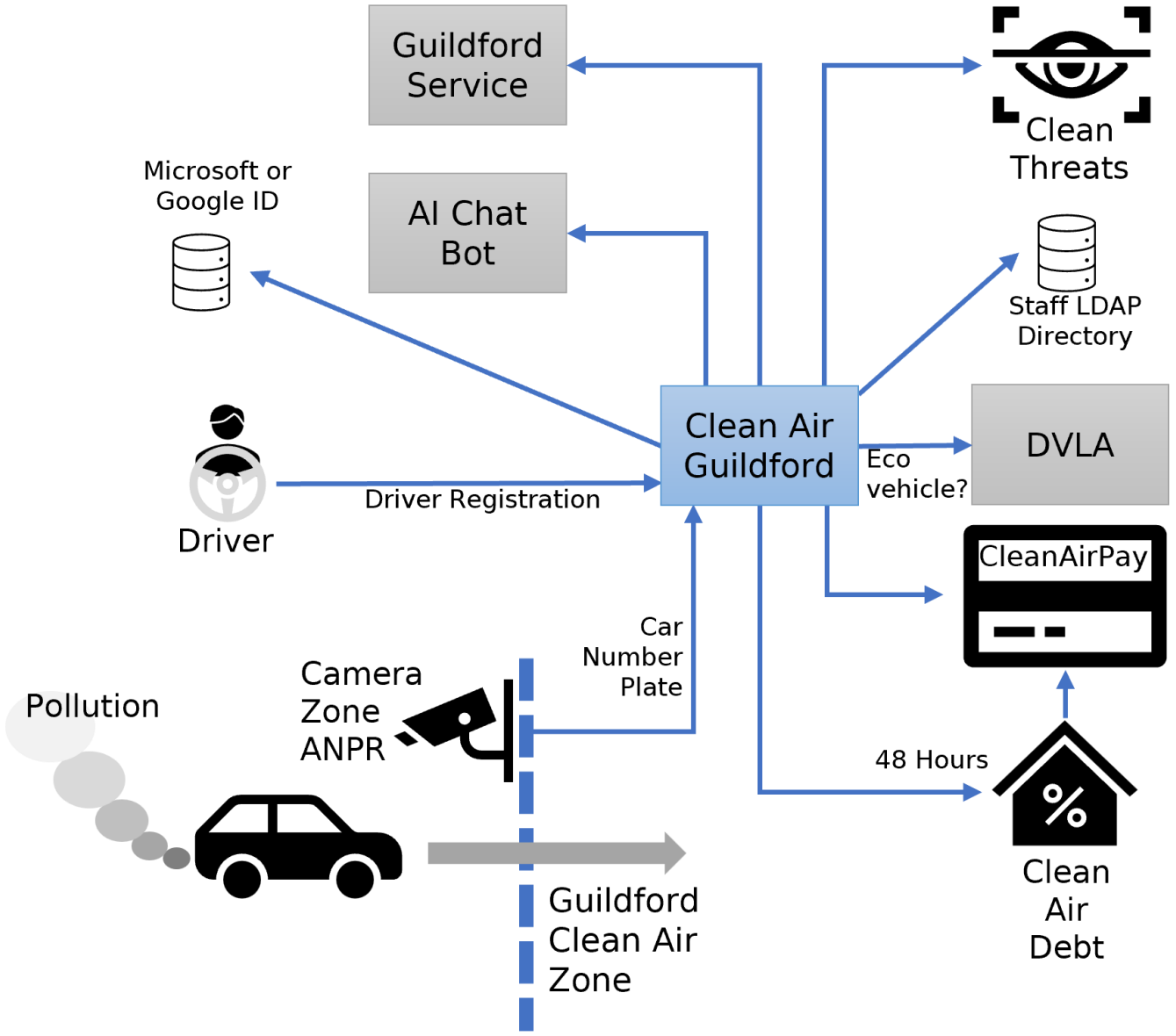


© Mark Buckwell, Carsten Horst and Stefaan Van daele

RSAC 2025 Conference

Clean Air Guildford Case Study

- Architecting an application to charge polluting vehicles to enter a city

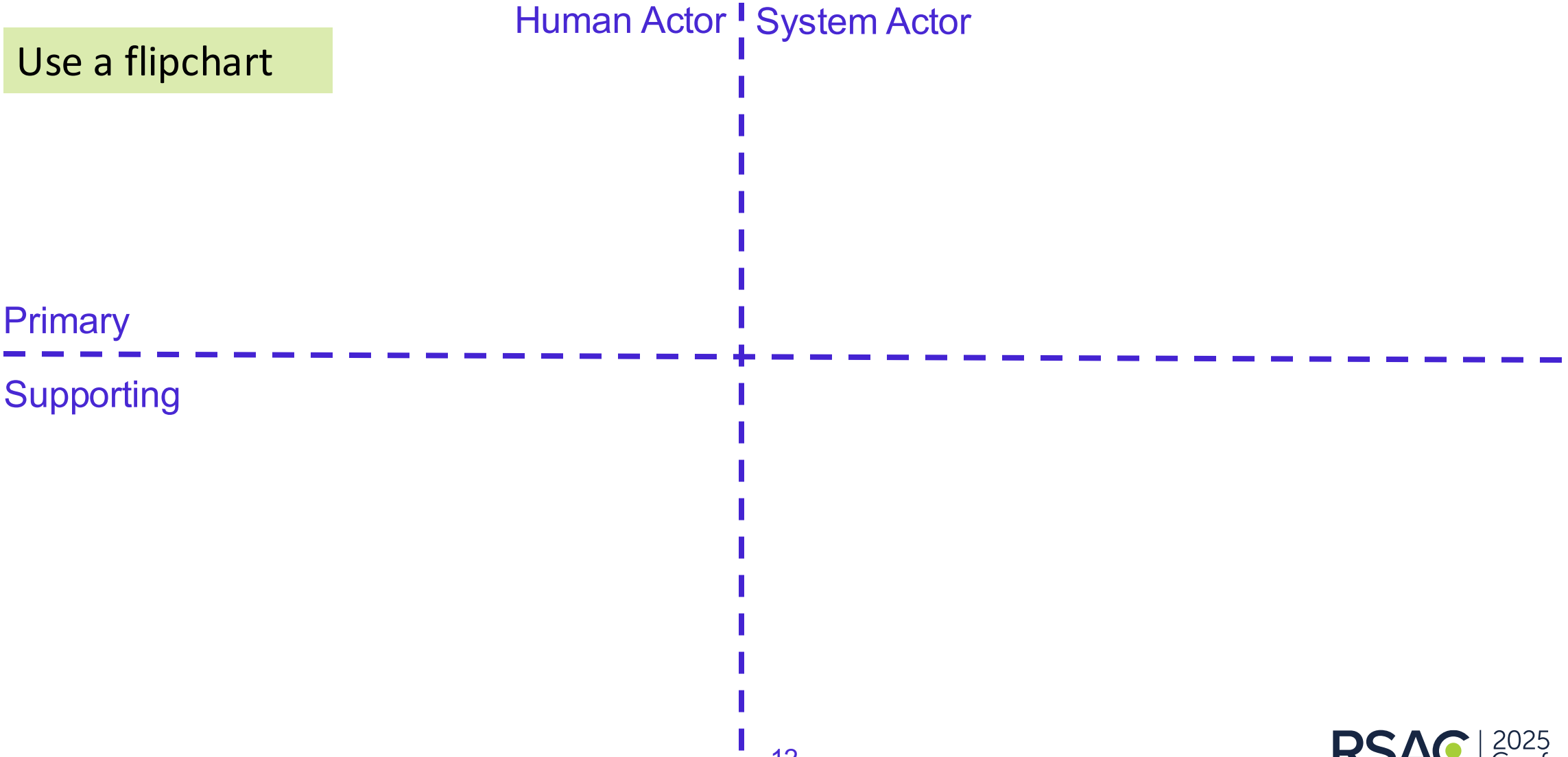


© Mark Buckwell, Carsten Horst and Stefaan Van daele

RSAC 2025 Conference

Team Exercise:
Identify the external actors for this application

Use a flipchart

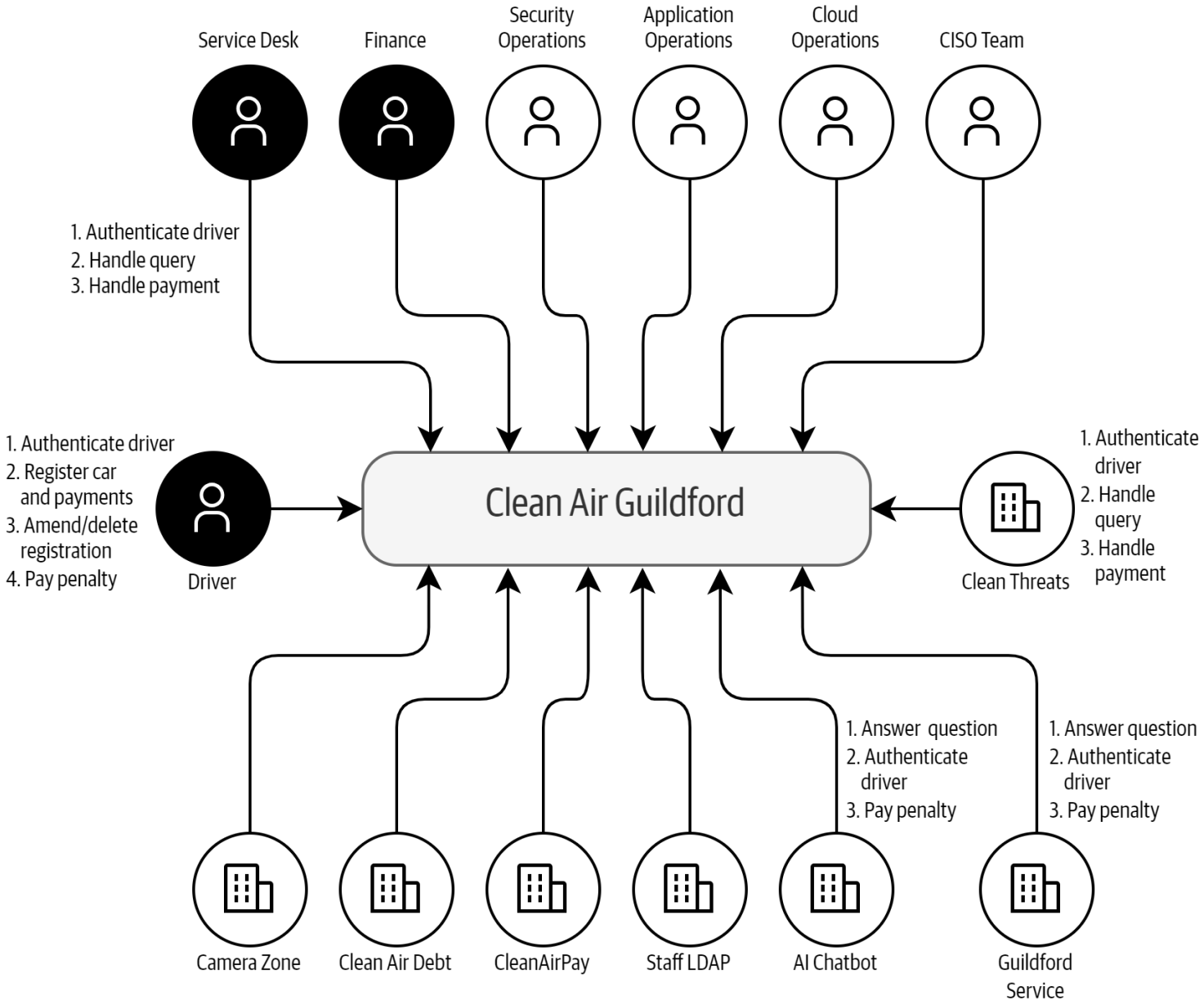


© Mark Buckwell, Carsten Horst and Stefaan Van daele

RSAC 2025 Conference

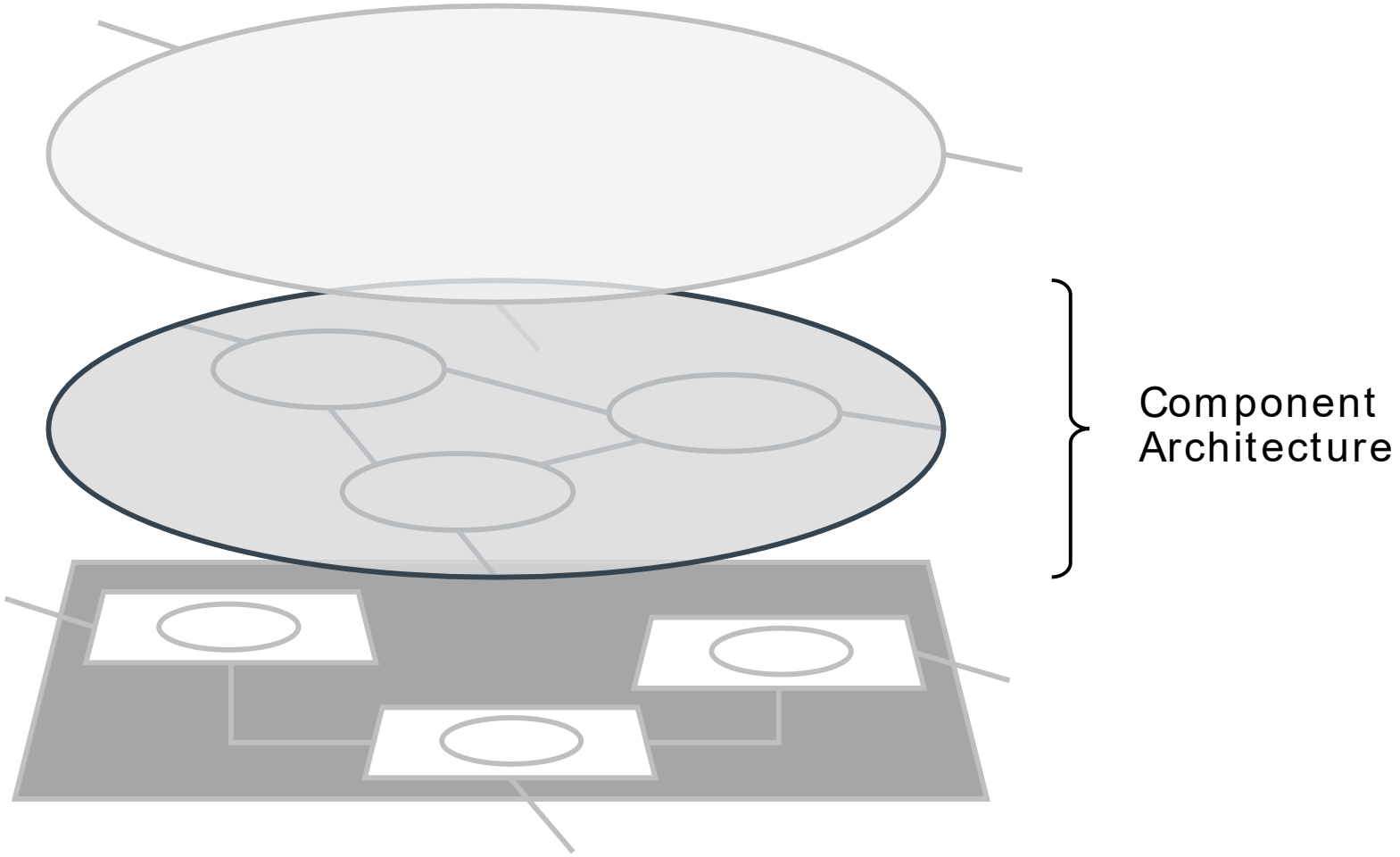
Stage 2 – Review and Layer 2

Clean Air Guildford System Context



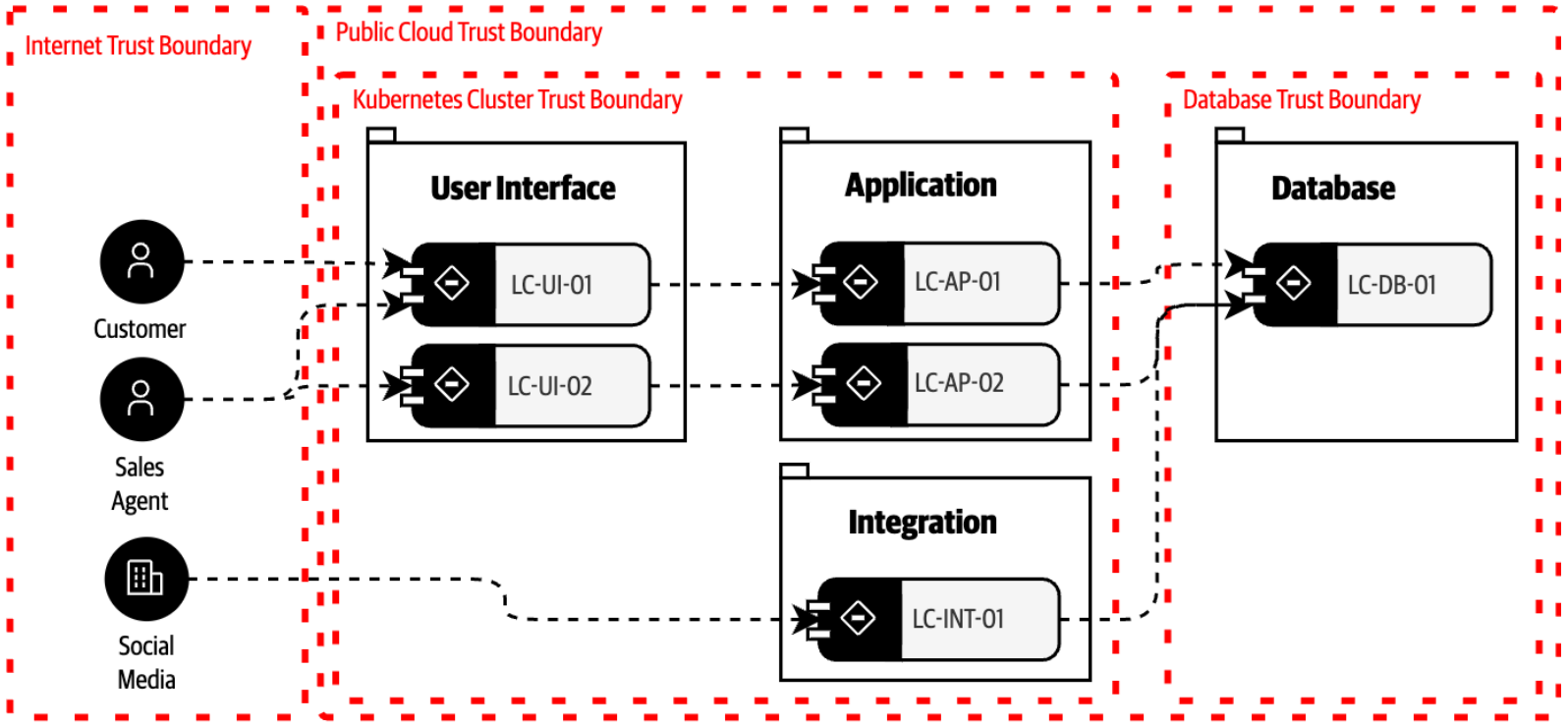
© Mark Buckwell, Carsten Horst and Stefaan Van daele

Next, we are going to examine the functional components inside the system boundary



© Mark Buckwell, Carsten Horst and Stefaan Van daele

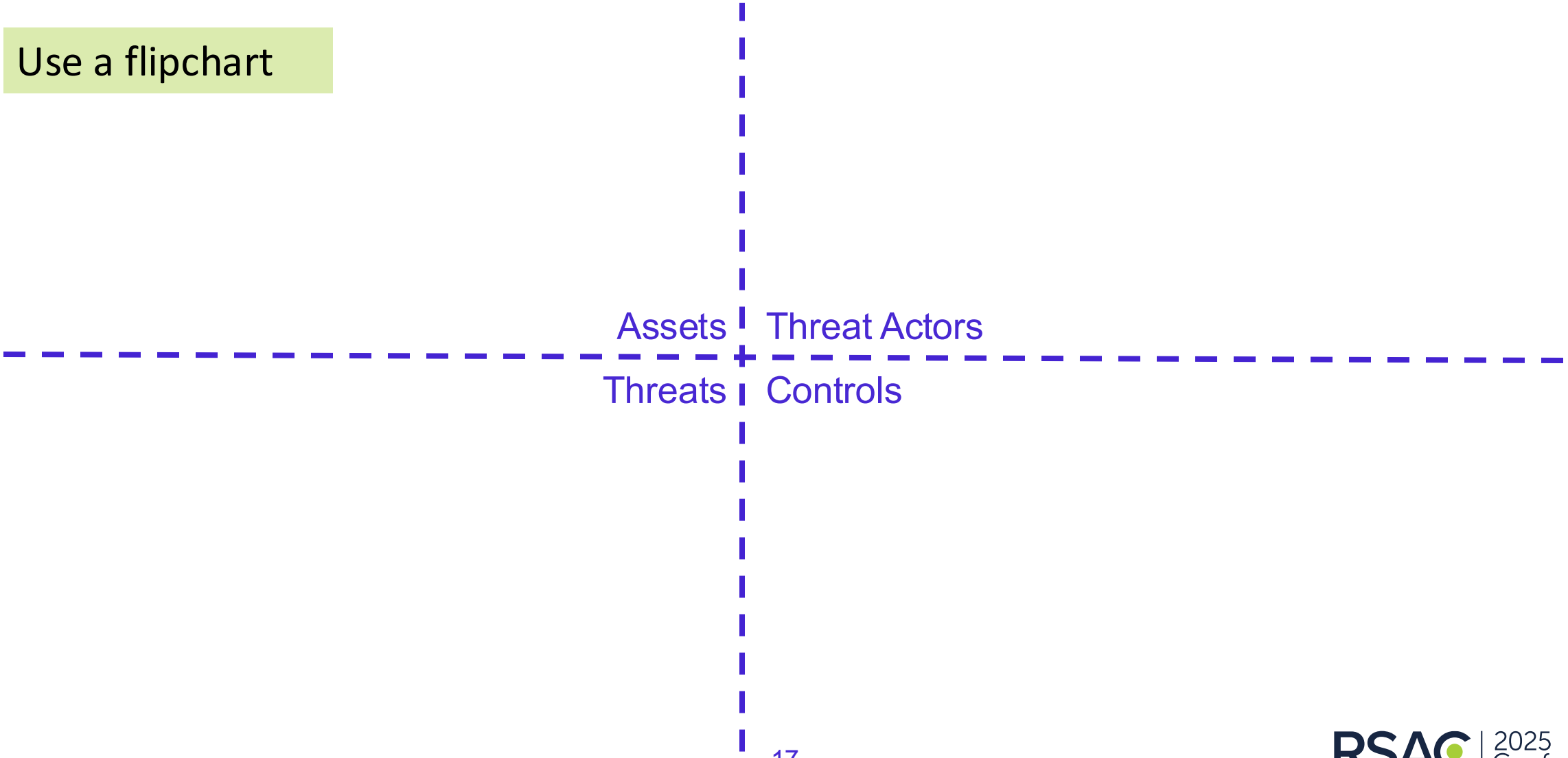
A component architecture diagram shows the functional components, subsystems and trust boundaries



© Mark Buckwell, Carsten Horst and Stefaan Van daele

Team Exercise:
Identify Assets, Threat Actors, Threats and Controls

Use a flipchart

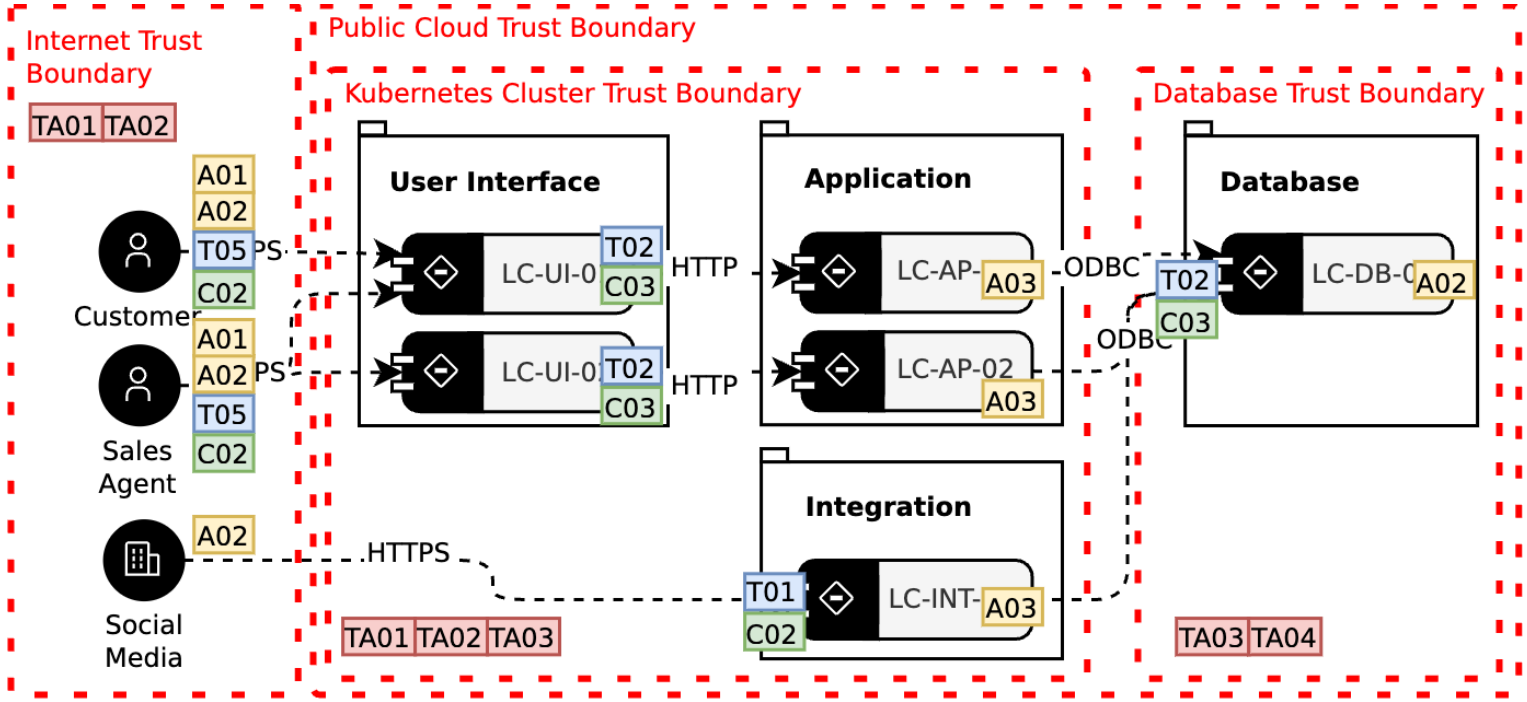


© Mark Buckwell, Carsten Horst and Stefaan Van daele

RSAC 2025 Conference

Stage 3 – Review and Layer 3

Complete the first stage of threat modelling, then move to the deployment of the functional components



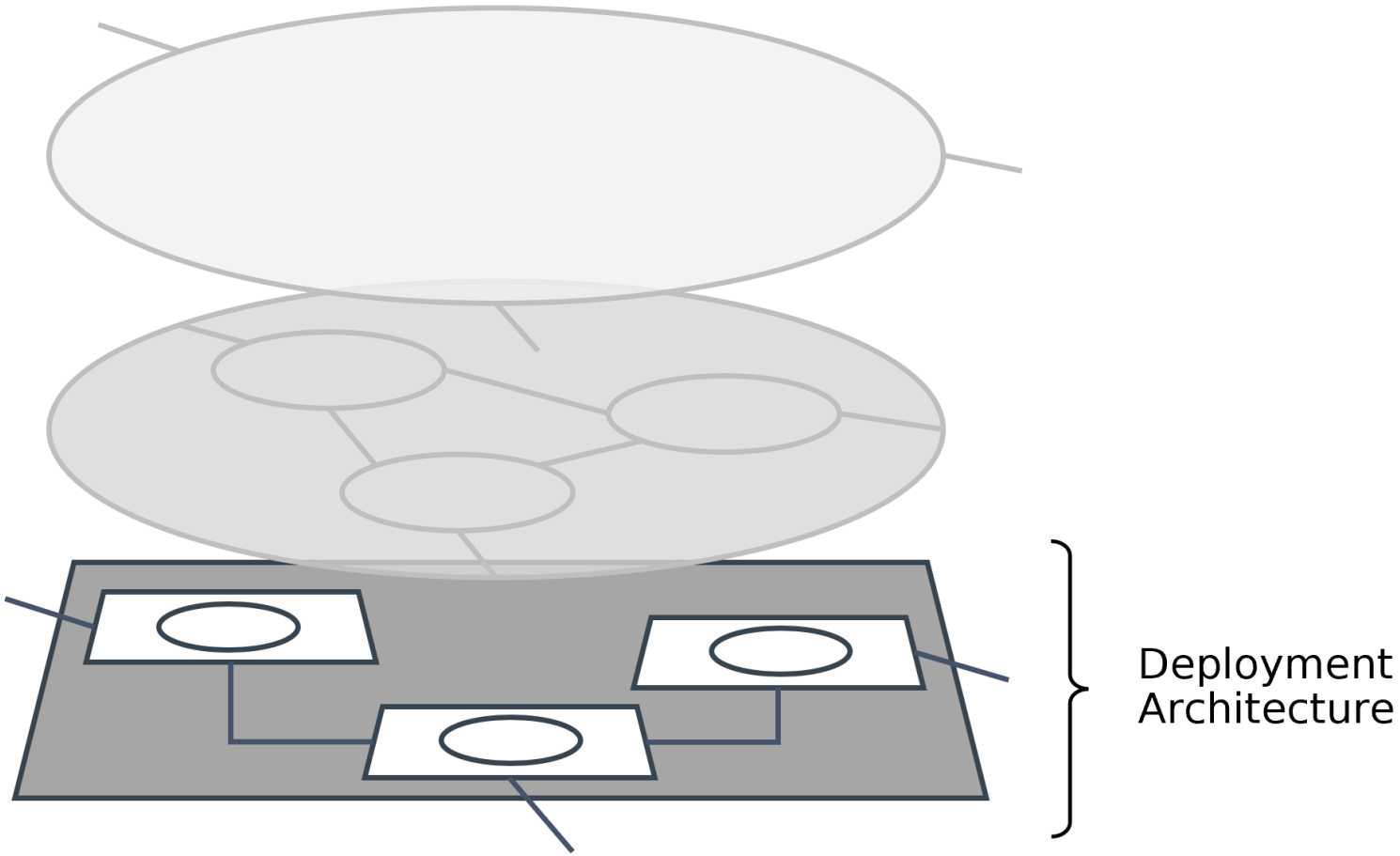
Assets	Threats
A01 - User Session ID A02 - Customer Information A03 - DB Access Credentials	T01 - Lack of IAM Controls T02 - missing sec. transp. layer T05 - Exploit of website vulns
Threat Actors	**Controls**
TA01 - External authorised TA02 - External unauthorised TA03 - Internal authorised TA04 - Internal unauthorised	C01 - Multi Factor Authentication C02 - Web Application Firewall C03 - Encryption

Component List
LC-UI-01 - Customer registration
LC-UI-02 - CRM UI
LC-AP-01 - Customer mgmt
LC-AP-02 - CRM Appl.
LC-DB-01 - CRM Database
LC-INT-01 - Social Media Integration

© Mark Buckwell, Carsten Horst and Stefaan Van daele

RSAC 2025 Conference

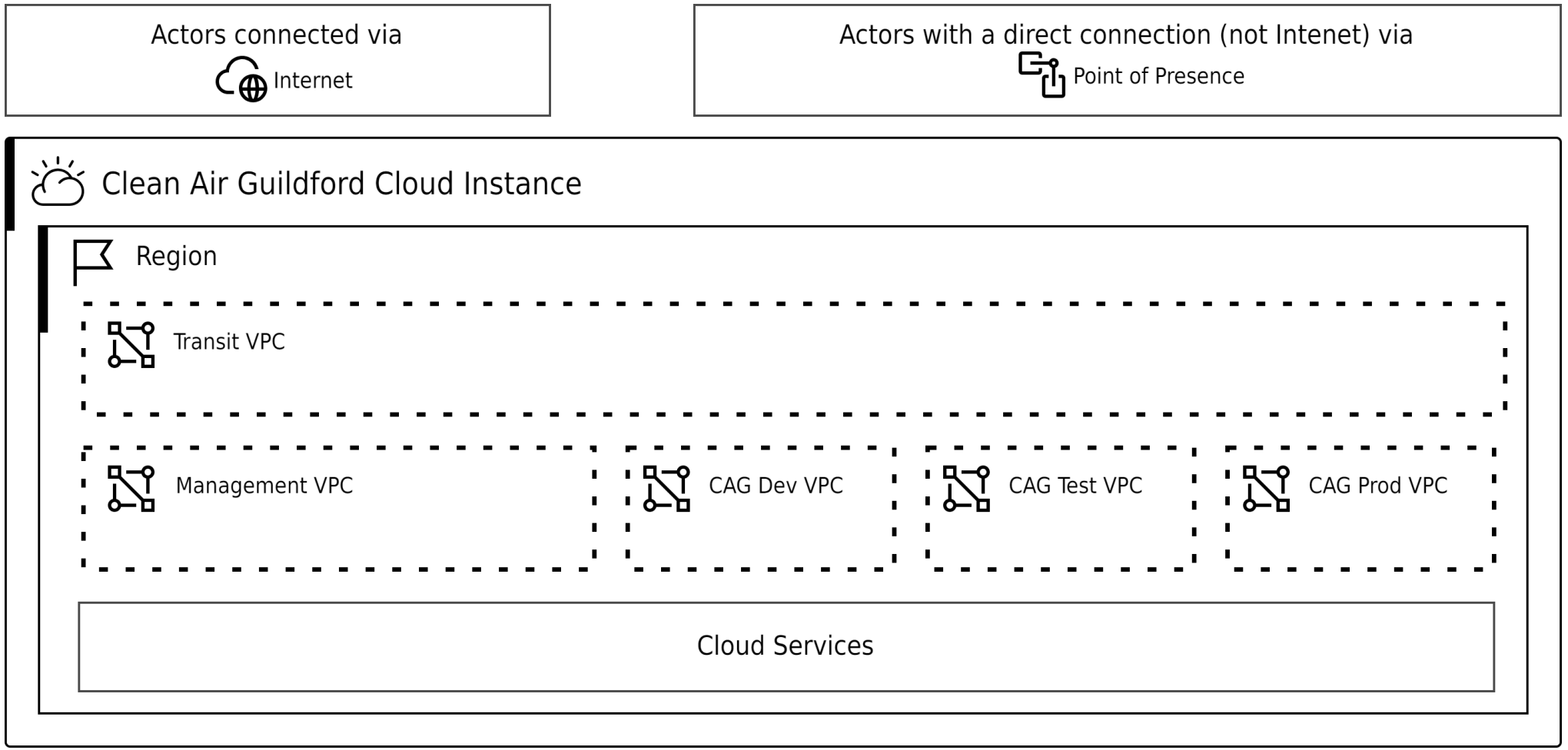
Next, we are going to examine the deployment of the functional components onto the infrastructure



© Mark Buckwell, Carsten Horst and Stefaan Van daele

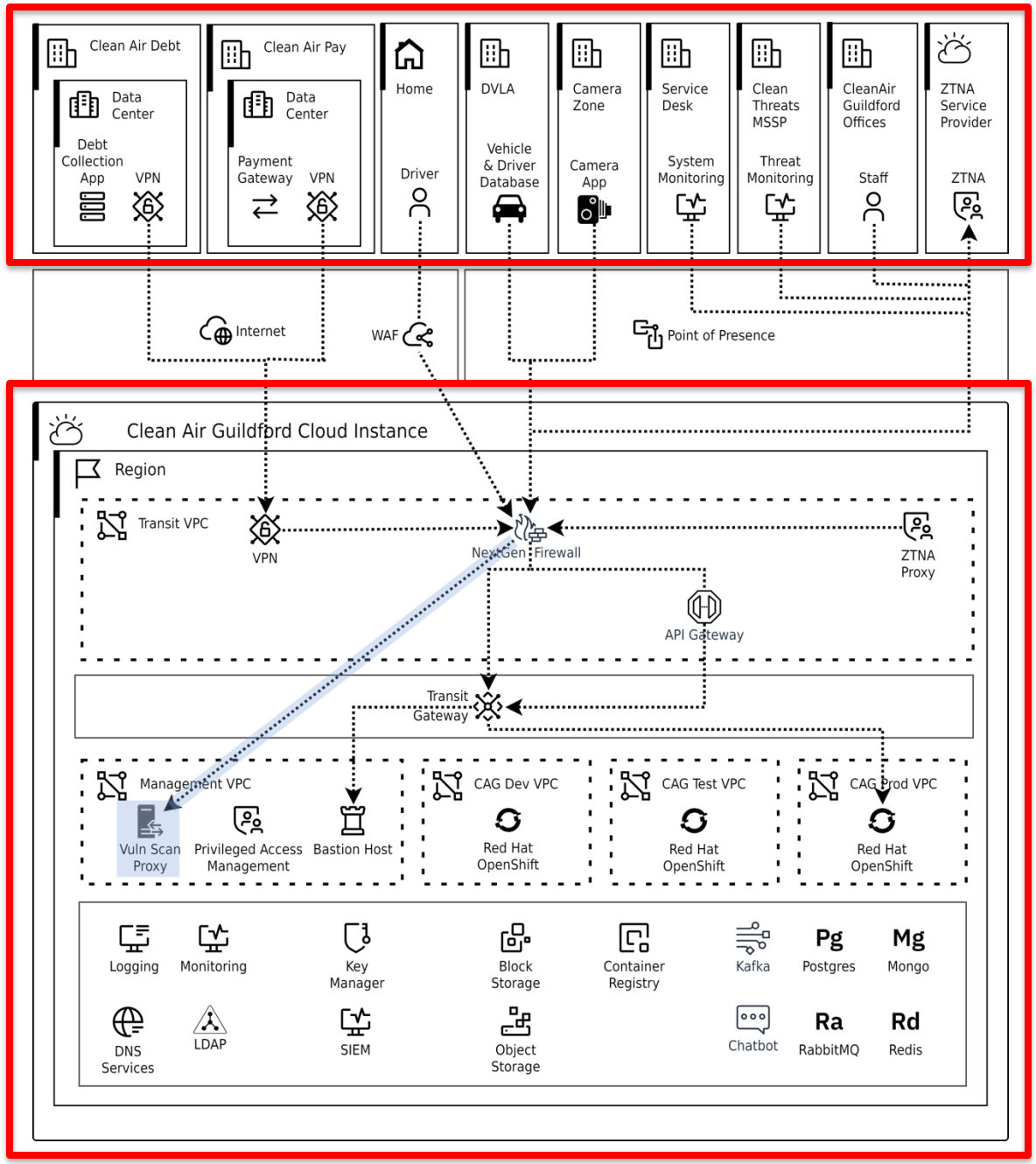
RSAC 2025 Conference

We start with a simple view of the deployment architecture for your workload



© Mark Buckwell, Carsten Horst and Stefaan Van daele

Complete the deployment architecture



Actors

System Context

System

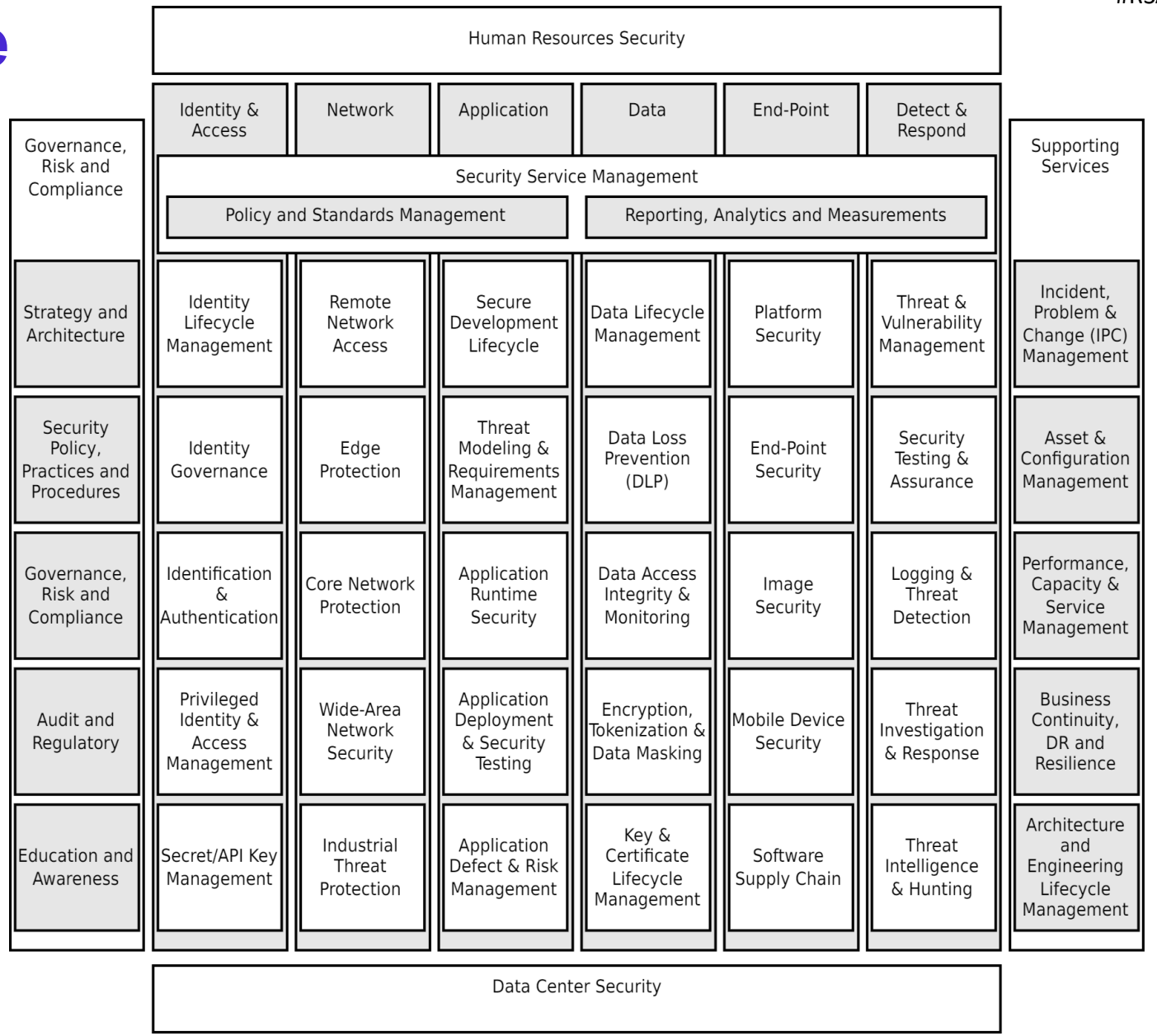
© Mark Buckwell, Carsten Horst and Stefaan Van daele

RSAC 2025 Conference

Guided by an Enterprise Security Architecture

Identify additional services needing integrating on the deployment architecture

Identity & Access	
Network	
Application	
Data	
End-Point	
Detect & Respond	

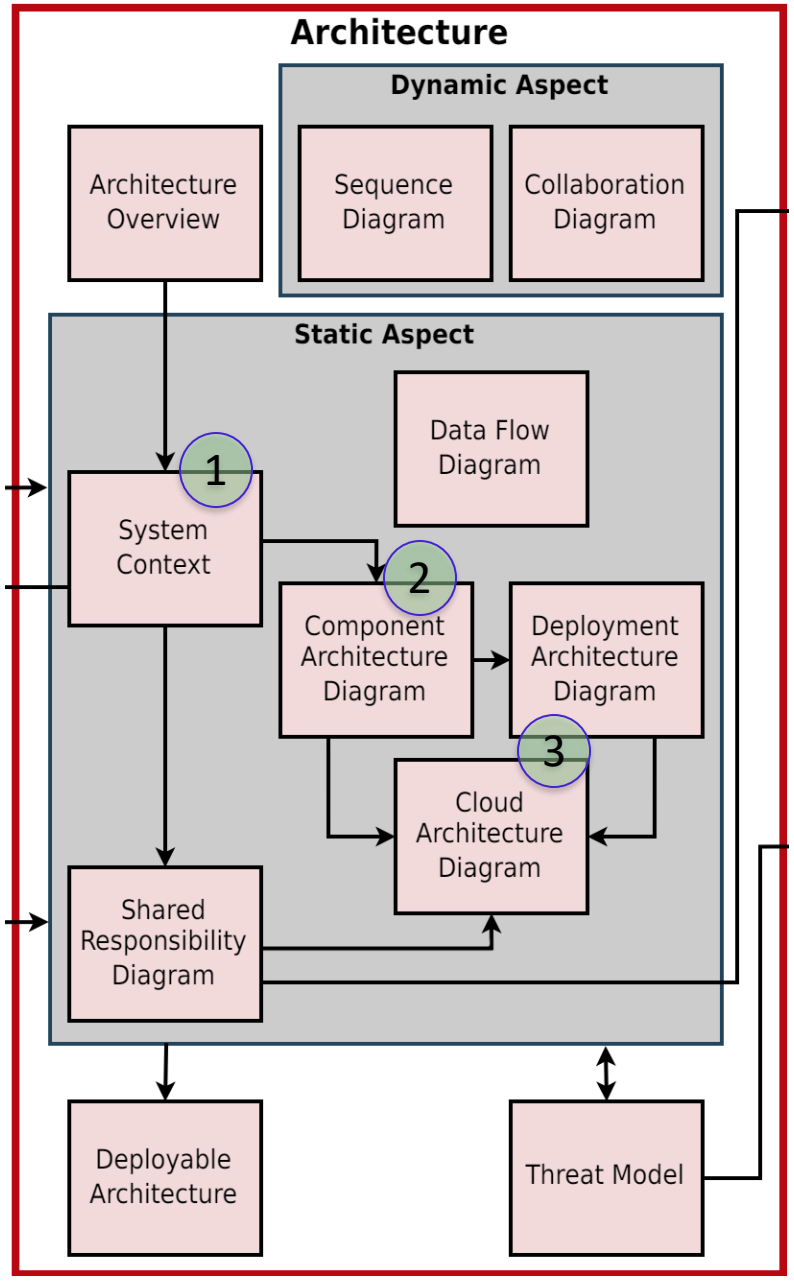


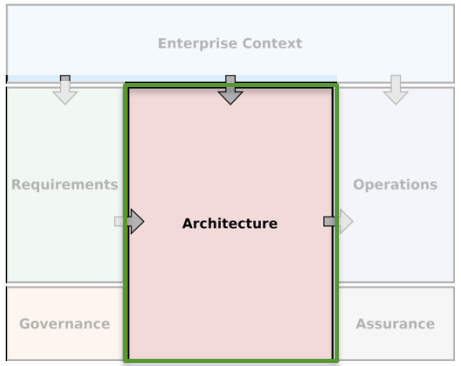
Use a flipchart

RSAC 2025 Conference

Stage 4 – Wrap Up

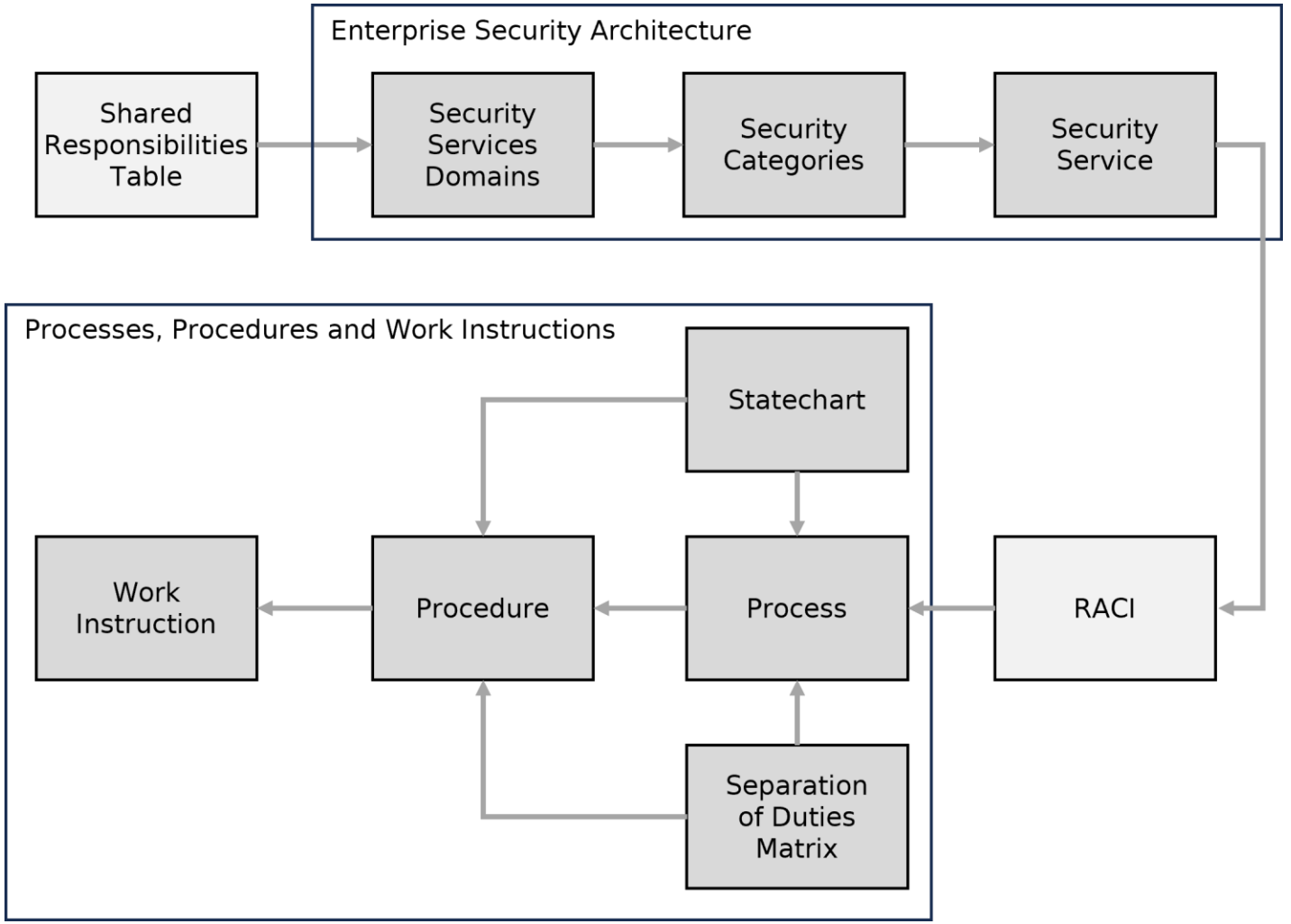
Building an architecture top down





#RSAC
RSAC 2025 Conference

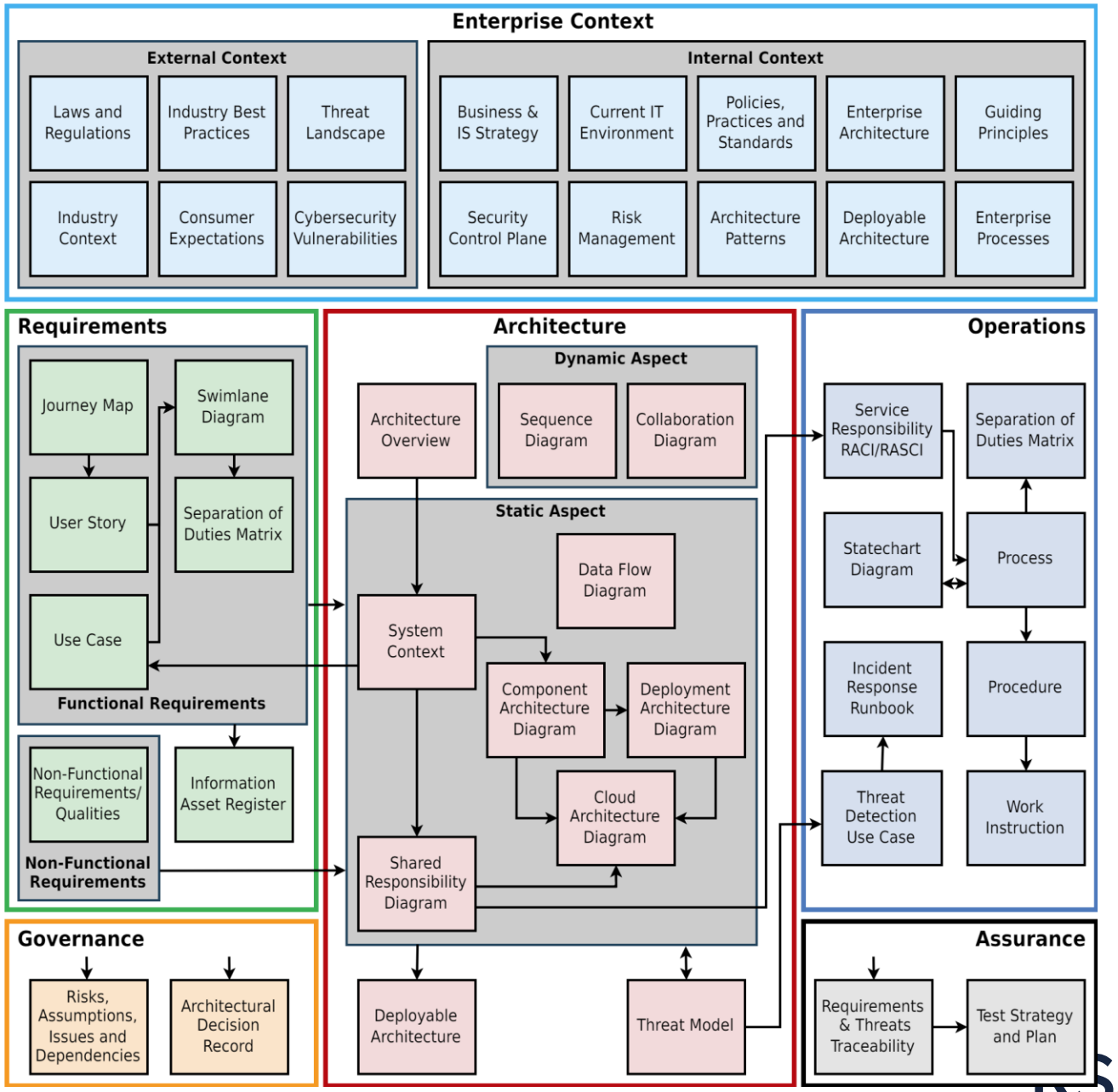
Take the identified security services and define RACIs, processes, procedures and work instructions



RSAC 2025 Conference

Artefact Dependency

There are additional artefacts that are part of the architectural thinking process

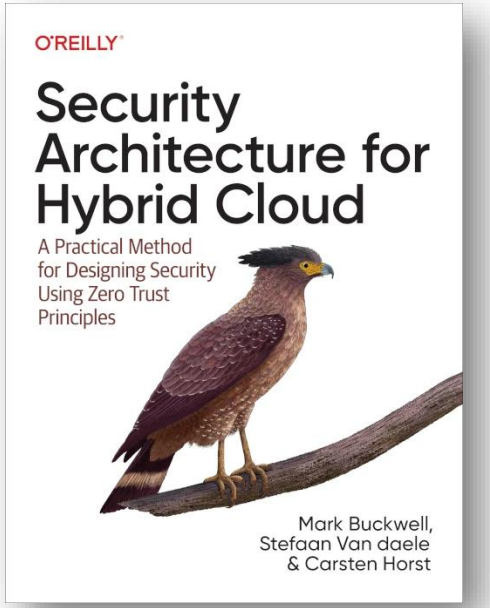


© Mark Buckwell, Carsten Horst and Stefaan Van daele

RSAC 2025 Conference

Apply What You Have Learned Today

- **Learn - this week**
  - Look at answers and further information https://securityarchitecture.cloud/rsac/25/answers
  - Listen to RSA Conference past contributions on security architecture
- **Review - in the next month or two**
  - Review chapters 5, 6, 8 and 9 in Security Architecture for Hybrid Cloud
  - Is your architectural thinking process more art than engineering?
    - Use the artifact dependency as a heatmap of activities performed today
    - Does ownership of artifacts extend to application and infrastructure architects?
    - Is there an architectural thinking for security champion?
- **Action - over the next year**
  - Integrate security artifacts into existing architectural thinking method
  - Perform method training with case study (not just click-and-test education)
  - Measure and improve architectural thinking for security practices
    - Use review techniques to assess extent of deployment


O'REILLY
Security Architecture for Hybrid Cloud
A Practical Method for Designing Security Using Zero Trust Principles
Mark Buckwell, Stefaan Van daele & Carsten Horst

RSAC™ | 2025 Conference

Many Voices.
One Community.